UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/409,617	10/01/1999	DAVID MICHAEL SHACKELFORD	TU9-99-029	5644

46917 7590 08/30/2006

KONRAD RAYNES & VICTOR, LLP.
ATTN: IBM37
315 SOUTH BEVERLY DRIVE, SUITE 210
BEVERLY HILLS, CA 90212

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 08/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/409,617
Filing Date: October 01, 1999
Appellant(s): SHACKELFORD, DAVID MICHAEL

David Victor
Reg. No. 39,867
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12 June 2006 appealing from the Office action mailed 13 December 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed..

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,473,692	DAVIS	12-1995
5,994,307	KOMURA	11-1999
6,195,432	TAKAHASHI	2-2001

Schneier, Applied Cryptography, Second Edition, 1996, John Wiley & Sons, Inc., page 45.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 2, 8-14, 16, 17, 21-28, 34-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent No. 5,473,692. Referring to claims 1, 16, 27, Davis discloses a system for computer software license enforcement wherein a certification agent contains a storage device of authentic key pairs (Col. 7, lines 30-64), which meets the limitation of a first computer system, maintaining keys of computer systems authorized to access software to be distributed. The hardware/first agent of the requester transmits an authentication device certificate to the certification system/second agent in order to access software (Col. 8, lines 33-36), which meets the limitation of a second computer system, receiving a request for software from a second computer system. The second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation of generating a message, encrypting the generated message, transmitting the encrypted message to the second computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of transmitting the encrypted message to the second computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response, decrypting the encrypted response with the determined key if there is one determined key. The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-

60), which meets the limitation of determining whether the decrypted response includes a part of the generated message transmitted to the second computer system. If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of the second computer system is authorized to access the software if the decrypted response includes the part of the generated message, permitting the second computer system access to the software after determination that the second computer system is authorized to access the software. If the response message does not match the original challenge then the communications are terminated and no valid license token is transmitted (Col. 8, lines 60-61), which meets the limitation of the second computer system is not authorized to access the software if the decrypted response does not include the part of the generated message transmitted to the second computer system.

Referring to claims 12, 25, Davis discloses a system for computer software license enforcement wherein a certification agent contains a storage device of authentic key pairs (Col. 7, lines 30-64). The key pairs are transmitted to the certification agent (Col. 7, lines 44-45), which meets the limitation of providing a key to the first computer system capable of decrypting an encrypted response from the second computer system. The hardware/first agent of the requester transmits an authentication device certificate to the certification system/second agent in order to access software (Col. 8, lines 33-36), which meets the limitation of transmitting a request for the software to the first computer system. The second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation of receiving an encrypted message from the first computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of processing the encrypted message to generate a response message including part of the encrypted message, encrypting the response message, transmitting the encrypted response message to the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of the encrypted response message is capable of being decrypted by the provided key at the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of receiving access to the requested software in response to the encrypted response message.

Referring to claims 2, 13, 17, 28, Davis discloses that the software being requested is a software application (Col. 9, lines 15-22), which meets the limitation of the software comprises software that is a member of a set of software types comprising computer programs, data, text, images, sound, and video.

Referring to claims 8, 9, 21, 22, 34, 35, Davis discloses that the second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of processing the encrypted response further comprises determining whether a message included in the encrypted response matches the generated message, wherein the second computer is authorized to access the software if the message included in the encrypted response matches the generated message, wherein the encrypting the message comprises encrypting the message with a private key of the first computer system that is the only key capable of being decrypted by a public key associated with the first computer system, wherein the second computer system maintains the public key that is capable of decrypting messages encrypted with the first computer system's private key, wherein the encrypted response received from the second computer system is encrypted with the second computer system's private key, wherein the maintained keys comprise public keys from the authorized computer systems, wherein processing the encrypted response further comprises decrypting the encrypted response with one of the maintained public keys.

Referring to claims 10, 23, 36, Davis discloses that the challenge also includes a digital certificate (Col. 8, lines 33-35), which meets the limitation of configuration data.

Referring to claims 11, 24, 37, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49), which meets the limitation the generated message is encrypted with a private key of the first computer system, wherein the first computer system maintains a private key that is the only key capable of being decrypted by a public key associated with the first computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54). The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of the encrypted response is encrypted with a private key of the second computer system, wherein the maintained keys comprise public keys from authorized computer systems.

Referring to claims 14, 26, 39, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49). The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of decrypting the received encrypted message with the public key associated with the first computer system that is the only key capable of decrypting messages encrypted with the first computer system's private key, encrypting the decrypted message with the second computer system's private key, transmitting the message encrypted with the second computer system's private key to the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58), which meets the limitation of wherein the key made available by the second computer system that is capable of decrypting the received encrypted response comprises the public key associated with the second computer system.

Referring to claim 38, Davis discloses a system for computer software license enforcement wherein a certification agent contains a storage device of authentic key pairs (Col. 7, lines 30-64). The hardware/first agent of the requester transmits an authentication device certificate to the certification system/second agent in order to access software (Col. 8, lines 33-36), which meets the limitation of transmitting a request for the software to the first computer system. The second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent.(Col. 8, lines 45-49), which meets the limitation of receiving an encrypted message from the first computer system. The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54), which meets the limitation of processing the encrypted message to generate a response message, transmitting the response message to the first computer system. The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of receiving access to the requested software in response to the response message.

Referring to claim 40, Davis discloses that the challenge also includes a digital certificate (Col. 8, lines 33-35), which meets the limitation of configuration data.

Claims 3, 18, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692. Referring to claims 3, 18, 29, Davis discloses that if the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22). Davis does not specify how the software is distributed. Davis does suggest that electronic distribution systems for software are a viable distribution option (Col. 2, lines 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to electronically distribute the actual software application at the time of authentication in the system of Davis in order to increase convenience and reduce distribution costs as taught by Davis (Col. 2, lines 27-29).

Claims 4, 15, 19, 30 and rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692, in view of Schneier. Referring to claims 4, 15, 19, 30, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49). The first agent receives and decrypts the encrypted challenge message and generates a response message by encrypting the decrypted challenge message and transmitting the encrypted response message to the second agent (Col. 8, lines 50-54). The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent decrypts the response message with the private key that corresponds to the first agent stored in the second agent storage device (Col. 8, lines 54-58). The second agent compares the original challenge message to the decrypted response message (Col. 8, lines 59-60). If the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22), which meets the limitation of determining whether the response includes the component included with the message. Davis does not disclose that the challenge is random. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the challenge in Davis to a random challenge in order for the challenge to be unpredictable as taught by Schneier (Page 45). According to Schneier (Page 45), it is computationally infeasible to predict what the next random bit will be, given complete knowledge of the algorithm or hardware generating the sequence and all of the previous bits in the stream. This is beneficial to Davis because the issuer of the challenge would want the challenge to be unpredictable so that the resultant authentication was genuine.

Claims 5, 6, 31, 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692, in view of Komura, U.S. Patent No. 5,994,307. Referring to claims 5, 6, 31, 32, Davis discloses that the second agent generates a challenge message, encrypts the message, and transmits the encrypted challenge message to the first agent (Col. 8, lines 45-49). Davis does not disclose that the challenge contains a time stamp. Komura discloses a packet transmission system wherein time stamp offset values are attached to data packets (message)(Col. 7, lines 22-30). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use time stamp offset values in the software licensing system of Davis, for synchronizing purposes taught in Komura (Col. 6, lines 40-67).

Claims 7, 20, 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis, U.S. Patent No. 5,473,692, in view of Takahashi, U.S. Patent No. 6,195,432. Referring to claims 7, 20, 33, Davis discloses that if the response message matches the original challenge, then the second agent transmits a valid license token to the first agent that allows the first agent to operate the software application (Col. 8, lines 60-65 & Col. 9, lines 15-22). Davis does not specify how the software is distributed. Davis does suggest that electronic distribution systems for software are a viable distribution option (Col. 2, lines 26-27). It would have been obvious to one of ordinary skill in the art at the time the invention was made to electronically distribute the actual software application at the time of authentication in the system of Davis in order to increase convenience and reduce distribution costs as taught by Davis (Col. 2, lines 27-29). Davis does not disclose or suggest that the software is automatically installed after electronic distribution. It would have been obvious to one of ordinary skill in the art to automatically install the transmitted software in Davis in order to assist users who are not accustomed to handle a personal computer as taught in Takahashi (Col. 3, lines 57-64).

(10) Response to Argument

Appellant's essential argument from pages 6-10 of the appeal brief is that Davis does not disclose the claimed "determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response." To avoid confusion, let the record show that the first node of Davis meets the claimed second computer system and the second node of Davis meets the claimed first computer system. The illustrative embodiment of Davis is shown on column 8, line 23 through column 9, line 26, which describes the first node (also called first hardware agent) requesting access to software from a second node (also called second hardware agent). The cited portion of Davis shows that the process for allowing the first node to access the software includes the second node transmitting an encrypted message to the first node (Col. 8, lines 46-49). The first node then decrypts the message, and generates a response message that is encrypted and then transmitted back to the second node (Col. 8, lines 49-54). The second node decrypts this message and compares the decrypted message with the message originally sent (Col. 8, lines 55-61) to determine whether the communication will continue. If the message is the same, communication is continued and the first node is ultimately granted software access (Col. 9, lines 15-18). Column 5, lines 31-61, of Davis disclose additional protocols that can be used for additional authentication (Col. 5, lines 8-10). Therefore, the procedures disclosed in column 5 of Davis are procedures that would be performed in addition to the procedure previously described. Column 5 discloses that the response message transmitted from the first node to the second node is encrypted with the private key of the first node (Col. 5, lines 37-42). Therefore, for the second node to decrypt the message, the second node has to have the public key of the first node to decrypt the message (Col. 5, lines 52-56). Davis never expressly discloses "a determination step" with respect to the public key of the first node. However, the disclosure on column 5 of Davis shows a procedure that meets the claimed determination step. The second node receives the public key of the first node from a trusted authority, and ultimately decrypts the encrypted message received from the first node (Col. 5, lines 47-56). This meets the claimed "determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response," because since the public key of the first node is received by the second node and used to ultimately decrypt an encrypted message, the public key of the first node is stored on the second node and is therefore considered maintained. Appellant's claims do not require the claimed first computer system to maintain a database of keys that are searched to find the key of the second computer system. Therefore, the second node storing the public key of the first node for future processing meets the claimed maintaining. Additionally, because the public key of the first node is being used to decrypt an encrypted message that was sent by the first node and encrypted with the private key of the first node, that public key of the first node would have been determined to be a maintained key for that first node that is capable of decrypted the received encrypted message. If the public key received by the second node was not the public key of the first node, the encrypted message would not have decrypted properly. In public key cryptosystems, data encrypted with a public key can only be decrypting that public key's corresponding private key, and visa versa. Therefore, the cited portions of Davis meets the claimed "determining whether there is one maintained key for the second computer system capable of decrypted the received encrypted response.

It is noted that independent claims 12 and 25 do not contain the claimed requirement of "determining whether there is one maintained key for the second computer system."

In response to appellant's argument that the references fail to show certain features of appellant's invention, it is noted that the features upon which appellant relies (i.e., the claim requirement of a first computer system that distributes software maintaining keys of computer systems authorized to access software to be distributed) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to appellant's arguments, the recitation "distributing computer software from a first computer system" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951). The body of the claims only requires "permitting the second computer system access to the software." The body of the claims does not include software distribution.

Appellant's argument that "Nowhere doe the cited Davis anywhere disclose that the second hardware agent doing the authentication, corresponding to the claimed first computer system, determine whether there is one key for the second computer system that can be used to decrypt the message and then decrypting the encrypted response from the claimed second computer system with that determined key," is not persuasive because, as stated above: the public key of the first node is stored in the second node for future processing and is considered maintained, and the public key of the first node is used to decrypt the encrypted message (encrypted by the private key of the first node), which meets the limitation of determining whether there is one maintained key for the second computer system capable of decrypted the received encrypted message.

Appellant's argument that "nowhere does the cited Davis anywhere disclose the claim requirement of determining a key for the second computer system to use to decrypt the message," is not persuasive and has been fully addressed above.

Appellant's argument that "there is no disclosure in this cited section (of Davis) of the claim requirement that the second node determine whether there is a key maintained for the second computer system to decrypt a received response, such that the second computer system is not allowed to access software if there is no determined key for the second computer system," is not persuasive because access to software is granted to the first node of Davis only if the message decrypted by the second node matches the message originally transmitted (Col. 5, lines 56-61 & Col. 8, lines 54-61). If the messages are not the same, communications are terminated, and no software access is granted. Therefore, if the second node does not have the public key of the first node stored for decryption of the receive message, communications with the first node will be terminated, which meets the limitation of determining whether there is a key maintained for the second computer system to decrypt a received response, such that the second computer system is not allowed to access software if there is no determined key for the second computer system.

Appellant's argument that "the second node does not maintain keys as claimed of system authorized to access software as claimed, because the second node obtains the public key of the first node from a trusted authority," is not persuasive because the second node stores the received key before processing (i.e. decrypting). Therefore, the second node would maintain the key received from the trusted authority.

Appellant's argument that the second node does not maintain keys (plural) is not persuasive because the background of Davis (Col. 1, lines 40-49) shows that Davis is concerned with authorized multiple nodes to access software. Therefore, the second node would receive multiple keys from the trusted authority, which would likewise be maintained by the second node.

Appellant's argument that "there is not disclosure that the cited second node considers the presence or absence of a key for the first node to determine whether to authorized the first node to access software," is not persuasive because that is not a claimed feature. The claims require, "determining whether there is one maintained key for the second computer system capable of decrypting the received encrypted response," which is met by Davis as shown above.

Appellant's argument that "the cited second hardware agent does not use the presence of a key maintained for the first hardware agent to determine whether access to software is permitted," is not persuasive because access to software is granted to the first node of Davis only if the message decrypted by the second node matches the message originally transmitted (Col. 5, lines 56-61 & Col. 8, lines 54-61). If the messages are not the same, communications are terminated, and no software access is granted. Therefore, if the second node does not have the public key of the first node stored for decryption of the receive message, communications with the first node will be terminated, which meets the limitation of determining whether there is a key maintained for the second computer system to decrypt a received response, such that the second computer system is not allowed to access software if there is no determined key for the second computer system.

Appellant's argument that "the presence of a key for the first hardware agent is not at issue in the cited col. 8 because the second hardware agent uses its own private key to decrypt the message, not a key maintained for the first hardware agent as claimed," is not persuasive because column 5, lines 31-61, of Davis disclose additional protocols that can be used for additional authentication (Col. 5, lines 8-10). Therefore, the procedures disclosed in column 5 of Davis are procedures that would be performed in addition to the procedures described in column 8. Column 5 shows the second node decrypting the encrypted message using the public key of the first node (Col. 5, lines 52-56).

Appellant's argument that the disclosed system of the Davis does not disclose determining whether a computer is authorized to access software is not persuasive because access to software is granted to the first node of Davis only if the message decrypted by the second node matches the message originally transmitted (Col. 5, lines 56-61 & Col. 8, lines 54-61). If the messages are not the same, communications are terminated, and no software access is granted. Therefore, if the second node does not have the public key of the first node stored for decryption of the receive message, communications with the first node will be terminated, which meets the limitation of determining whether there is a key maintained for the second computer system to decrypt a received response, such that the second computer system is not allowed to access software if there is no determined key for the second computer system.

Appellant's argument that "Nowhere does the cited Davis disclose that the first hardware agent encrypts the challenge message that can be decrypted with a key the first hardware agent provided to the second hardware agent," is not persuasive because the claims do not require that the key, used to decrypt the encrypted message, be transmitted directly from the claimed second computer system to the claimed first computer system. Claims 12 and 25 require the key to be provided at the claimed first computer system. Claim 26 requires that the key be made available by the second computer system. In Davis, the trusted authority would have to receive the public key of the first node from the public key. Therefore, the claims do not require a direct transmission of the key from the claimed second computer system to the claimed first computer system.

Appellant's argument that "nowhere does the cited Davis disclose that he second hardware agent maintain public keys from multiple authorized first hardware agents to use to decrypt their challenge response," is not persuasive because the background of Davis (Col. 1, lines 40-49) shows that Davis is concerned with authorized multiple nodes to access software. Therefore, the second node would receive multiple keys from the trusted authority, which would likewise be maintained by the second node.

Appellant's argument that "Nowhere does this cited col. 8 anywhere disclose that the message sent with the authentication certificate include a request for configuration data from the second hardware agent, such that a determination is made whether the configuration data is for a system that is authorized to access the software," is not persuasive because the claims require the request for configuration data to come from the claimed second computer system (which correlates to the first node in Davis). Regardless, Davis discloses that the first node transmits a message containing the first node certificate to the second node, and the second node responds by transmitted a message with the second node certificate (Col. 8, lines 33-44). The certificate is used as configuration data because the certificate includes key data that maintains communications (Col. 5, lines 47-52 & Col. 8, lines 54-58). The first message with first node certificate would be considered a request because the second node would have the first node key data, and would realize that to communicate their certificate with key data (second node certificate) would have to be transmitted to the first node.

In response to appellant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Benjamin E. Lanier

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu KV

Christopher Revak